

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Yves AUDEBERT

Application No.: To Be Assigned

Filed: November 28, 2000

For: DATA PROCESSING SYSTEM FOR APPLICATION TO ACCESS BY  
ACCREDITATION

CLAIM FOR PRIORITY

Assistant Commissioner of Patents  
Washington, D.C. 20231

Dear Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

French Appln. No. 9915980, Filed December 17, 1999.

In support of this claim, a certified copy of said original foreign application is filed herewith.

JC853 U.S. PTO  
09/723284

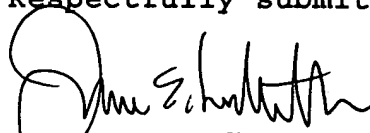


#2

This Page Blank (uspto)

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,



Date: November 28, 2000

James E. Ledbetter  
Registration No. 28,732

JEL/ejw

ATTORNEY DOCKET NO. L741.00101

STEVENS, DAVIS, MILLER & MOSHER, L.L.P.

1615 L Street, NW, Suite 850

P.O. Box 34387

Washington, DC 20043-4387

Telephone: (202) 408-5100

Facsimile: (202) 408-5200

**This Page Blank (uspto)**

JC053 U.S. PTO  
09/723284  
11/28/00

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 02 OCT. 2000

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

Best Available Copy

INSTITUT	SIEGE
NATIONAL DE	26 bis, rue de Saint Petersburg
LA PROPRIÉTÉ	75800 PARIS Cédex 08
INDUSTRIELLE	Téléphone : 01 53 04 53 04
	Télécopie : 01 42 93 59 30

**This Page Blank (uspto)**

<b>REMISE DES PIÈCES</b> DATE <b>17 DEC 1999</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE <b>9915980</b> PAR L'INPI <b>17 DEC. 1999</b>		<b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE</b> À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE <b>CABINET de BOISSE ET COLAS</b> CONSEILS en PROPRIÉTÉ INDUSTRIELLE 37, Avenue Franklin-Roosevelt 75008 PARIS	
<b>Vos références pour ce dossier</b> (facultatif) JPC/LT/137629/D.2735			
<b>Confirmation d'un dépôt par télécopie</b> <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
<b>2 NATURE DE LA DEMANDE</b>		<b>Cochez l'une des 4 cases suivantes</b>	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N°	Date <input type="text"/>
		N°	Date <input type="text"/>
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/>	Date <input type="text"/>
		N°	Date <input type="text"/>
<b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b> SYSTEME INFORMATIQUE POUR APPLICATION A ACCES PAR ACCREDITATION			
<b>4 DÉCLARATION DE PRIORITÉ</b> <b>OU REQUÊTE DU BÉNÉFICE DE</b> <b>LA DATE DE DÉPÔT D'UNE</b> <b>DEMANDE ANTÉRIEURE FRANÇAISE</b>		Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
<b>5 DEMANDEUR</b>		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		ACTIVCARD	
Prénoms			
Forme juridique		société anonyme	
N° SIREN		3 . 4 . 1 . 2 . 1 . 3 . 4 . 1 . 1	
Code APE-NAF			
Adresse	Rue	24-28, avenue du Général de Gaulle	
	Code postal et ville	92156 SURESNES CEDEX	
Pays		FRANCE	
Nationalité		française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

REMISE DES PIÈCES DATE <b>17 DEC 1999</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI		DB 540 W / 260899	
Vos références pour ce dossier : (facultatif)			JPC/LT/R137629/D.2735		
<b>6 MANDATAIRE</b>					
Nom					
Prénom					
Cabinet ou Société					
CABINET DE BOISSE ET COLAS					
N° de pouvoir permanent et/ou de lien contractuel					
Adresse		Rue	37, avenue Franklin D. Roosevelt		
		Code postal et ville	75008	PARIS	
N° de téléphone (facultatif)					
N° de télécopie (facultatif)					
Adresse électronique (facultatif)					
<b>7 INVENTEUR (S)</b>					
Les inventeurs sont les demandeurs			<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée		
<b>8 RAPPORT DE RECHERCHE</b>			Uniquement pour une demande de brevet (y compris division et transformation)		
Établissement immédiat ou établissement différé			<input checked="" type="checkbox"/> <input type="checkbox"/>		
Paiement échelonné de la redevance			Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non		
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>			Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):		
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes					
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire)  J.P. COLAS - CPI N° 92-1056			VISA DE LA PRÉFECTURE OU DE L'INPI		

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.  
 Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.



DÉPARTEMENT DES BREVETS

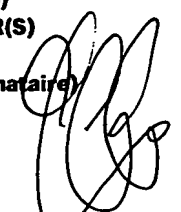
26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.  
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W / 260899

<b>Vos références pour ce dossier</b> (facultatif)		JPC/LT/R137629/D.2735	
<b>N° D'ENREGISTREMENT NATIONAL</b>		991.5580	
<b>TITRE DE L'INVENTION</b> (200 caractères ou espaces maximum)  SYSTEME INFORMATIQUE POUR APPLICATION A ACCES PAR ACCREDITATION			
<b>LE(S) DEMANDEUR(S) :</b>  ACTIVCARD 24-28, avenue du Général de Gaulle 92156 SURESNES CEDEX FRANCE			
<b>DESIGNE(NT) EN TANT QU'INVENTEUR(S) :</b> (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
<b>Nom</b>		AUDEBERT	
<b>Prénoms</b>		Yves	
<b>Adresse</b>	<b>Rue</b>	237 Forrester Road	
	<b>Code postal et ville</b>	95032	LOS GATOS CA - U.S.A.
<b>Société d'appartenance</b> (facultatif)			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance</b> (facultatif)			
<b>Nom</b>			
<b>Prénoms</b>			
<b>Adresse</b>	<b>Rue</b>		
	<b>Code postal et ville</b>		
<b>Société d'appartenance</b> (facultatif)			
<b>DATE ET SIGNATURE(S)</b> <b>DU (DES) DEMANDEUR(S)</b> <b>OU DU MANDATAIRE</b> (Nom et qualité du signataire) Le 17 décembre 1999  J.P. COLAS CPI N° 92 1056			

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.  
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

L'invention concerne des perfectionnements apportés aux systèmes informatiques dans lesquels l'accès d'un utilisateur à un ou plusieurs logiciels, par exemple des applications, est commandé par une ou plusieurs données accréditives.

5 La sécurité d'un système informatique, en particulier la sécurité de l'accès à des logiciels tels que des systèmes d'exploitation ou des applications (banque à domicile, commerce électronique, etc...) repose sur une authentification de l'utilisateur au moyen de données accréditives statiques qui, le plus souvent, consistent en un nom attribué à l'utilisateur ("login name") et un  
10 mot de passe statique.

Dans la suite, on entend par système informatique n'importe quel système comprenant un ordinateur personnel, un téléphone, un téléphone mobile, un assistant numérique personnel etc... permettant à un utilisateur d'exécuter, soit une application locale, soit la partie client d'une application, par  
15 exemple dans le cadre d'une architecture client-serveur.

Différents protocoles d'authentification basés sur la connaissance d'un mot de passe statique par un utilisateur sont connus :

- authentification de base : le mot de passe est transmis en clair à un module d'authentification côté serveur ;
- 20 - mot de passe chiffré : une clé de session est transmise en utilisant un algorithme à clé publique ( par exemple de type DIFFIE-HELLMAN), ce qui permet d'établir un canal sécurisé entre deux entités, via lequel sera transmis le mot de passe, sans qu'il soit nécessaire que celles-ci partagent préalablement un mot de passe secret ;
- 25 - authentification par condensé : la partie client de l'application chiffre le mot de passe (ou un condensé du mot de passe) au moyen d'un aléa envoyé par le module d'authentification côté serveur ;
- Kerberos : les données accréditives sont transmises à l'utilisateur par le module d'authentification côté serveur, sous forme chiffrée au moyen du mot de  
30 passe de l'utilisateur, de sorte que seul ce dernier a le moyen d'utiliser les données accréditives.

Cependant, ces mots de passe statiques sont vulnérables sur de nombreux points car ils peuvent être divulgués (mot de passe porté licitement ou frauduleusement à la connaissance d'une tierce personne), cassés lorsqu'ils  
35 sont faibles (mot de passe utilisé répétitivement sans modification, mot de passe court, attaque au dictionnaire), découverts par espionnage d'une ligne de communication ou émulation d'un serveur d'authentification, ou encore rejoués en reproduisant une séquence d'authentification.

Pour remédier à ces inconvénients, il est connu de faire appel à d'autres mécanismes offrant une plus grande sécurité que les mots de passe statiques.

Une première solution connue consiste à utiliser des mots de passe dynamiques, c'est-à-dire des mots de passe qui sont modifiés à chaque utilisation. Ces mots de passe dynamiques peuvent être du type synchrone (c'est-à-dire qu'ils sont modifiés de manière synchrone côté utilisateur et côté serveur, par exemple en fonction du temps et/ou du nombre d'utilisations) ou asynchrones (à chaque requête d'accès, le module d'authentification côté serveur génère un aléa ou challenge différent qui est transmis côté utilisateur pour générer le mot de passe dynamique au moyen d'un algorithme approprié). Dans l'un ou l'autre cas (mots de passe synchrones et asynchrones), des clés secrètes sont partagées côté serveur et côté utilisateur. Côté utilisateur, les mots de passe dynamiques peuvent être générés par un dispositif de sécurité personnel (PSD) tel qu'une carte à puce, un dispositif électronique portable et sécurisé ("token"), etc....

Une autre solution fait appel à des systèmes de cryptographie à clé publique, l'utilisateur possédant une clé privée et la clé publique étant certifiée par une autorité de certification. Une séquence d'authentification au moyen d'un tel système peut se dérouler de la manière suivante :

- l'utilisateur transmet un certificat (contenant son nom d'utilisateur, sa clé publique, son adresse, etc....) au serveur ;
- à réception du certificat, le module d'authentification du serveur génère et envoie à l'utilisateur un aléa ;
- l'utilisateur signe l'aléa au moyen de sa clé privée ;
- le module d'authentification vérifie l'aléa signé au moyen de la clé publique et authentifie l'utilisateur s'il y a cohérence.

Lorsqu'elles sont utilisées, ces solutions à mot de passe dynamique ou clé publique remplacent les mécanismes d'authentification basés sur un mot de passe statique ou font appel à un serveur d'authentification externe.

Il est également connu de faire appel à un serveur de mot de passe (SSO) au moyen duquel, par un processus unique d'authentification et d'autorisation, un utilisateur peut accéder à tous les calculateurs et systèmes auxquels il est autorisé à accéder, sans avoir besoin d'introduire de nombreux mots de passe différents. Une fois que l'utilisateur est authentifié, à savoir par une authentification faisant appel à un mot de passe fort (mot de passe comportant un grand nombre de caractères), il peut demander au serveur de mot de passe l'exécution d'une application. Le serveur de mot de passe charge alors dans le terminal de l'utilisateur un ensemble de données comprenant les

données accréditives de l'utilisateur pour l'application requise, ce qui permet au terminal de lancer l'exécution de l'application. Néanmoins, cette solution nécessite un serveur d'authentification spécifique (SSO) et repose néanmoins sur une première authentification de l'utilisateur vis-à-vis de ce serveur sur la

5 base d'un mot de passe statique.

L'invention vise à améliorer la sécurité des mécanismes par lesquels, au moyen de données accréditives statiques (nom d'utilisateur, mot de passe, etc...), un utilisateur doté d'un terminal peut s'authentifier vis-à-vis d'un logiciel exécuté soit localement dans ce terminal, soit pour partie dans ce terminal et

10 dans un serveur auquel ce terminal est connecté.

Un autre but de l'invention est de fournir un système informatique comportant des mécanismes perfectionnés de contrôle d'accès à une ou plusieurs applications et dans lequel, en outre, le protocole d'authentification basé sur le partage d'une donnée accréditive secrète et statique entre le côté

15 client et le côté serveur d'une application n'est pas modifié et le module d'authentification de l'application côté serveur demeure inchangé.

A cet effet, l'invention a pour objet un système informatique pour l'exécution d'au moins un logiciel dont l'accès par un utilisateur est commandé par la fourniture d'au moins une donnée accréditive attribuée audit utilisateur, le

20 dit système comprenant :

- au moins un terminal comportant des moyens de traitement de données pour l'exécution dudit logiciel au moins en partie,
- des premiers moyens de mémorisation associés audit logiciel pour le
- 25 stockage d'au moins une première donnée accréditive propre audit utilisateur,
- des moyens de contrôle d'accès pour autoriser l'accès audit logiciel en réponse à une cohérence entre ladite première donnée accréditive stockée dans lesdits premiers moyens de mémorisation et une seconde donnée accréditive appliquée via ledit terminal audit logiciel,

caractérisé en ce que ledit système comprend :

- 30 - au moins un dispositif de sécurité personnel audit utilisateur, associé audit terminal, et comportant des seconds moyens de mémorisation pour le stockage sécurisé de ladite seconde donnée accréditive,

et en ce que ledit terminal comprend au moins en partie des moyens de gestion de données accréditives comportant :

- 35 - des moyens de lecture et de transmission de donnée accréditive pour lire ladite seconde donnée accréditive stockée dans lesdits seconds moyens de mémorisation la transmettre auxdits moyens de contrôle d'accès en réponse à la présentation d'une demande d'accès audit logiciel, et

- des moyens de mise à jour de données accréditives pour commander sélectivement la génération et le chargement dans lesdits premiers et lesdits seconds moyens de mémorisation respectivement d'une nouvelle donnée accréditive en remplacement de la donnée accréditive précédemment mémorisée.

5

De préférence, le système informatique selon l'invention comprend en outre une ou plusieurs des caractéristiques suivantes considérées seules ou en combinaison :

- lesdits moyens de contrôle d'accès sont adaptés pour autoriser l'accès audit logiciel en réponse à une identité entre lesdites première et seconde données accréditives,
- lesdits seconds moyens de mémorisation sont adaptés pour stocker un premier code d'identification dudit utilisateur, ledit terminal comprend des moyens d'interface pour l'application d'un second code d'identification audit dispositif de sécurité personnel, et l'accès audit dispositif personnel de sécurité étant autorisé en réponse à une identité entre lesdits premier et second codes d'identification,
- lesdits moyens de mise à jour de données accréditives sont adaptés pour générer automatiquement et transmettre ladite nouvelle donnée accréditive directement auxdits premiers et seconds moyens de mémorisation, sans communication de ladite nouvelle donnée accréditive audit utilisateur,
- lesdits moyens de gestion de données accréditives sont des moyens logiciels faisant partie dudit logiciel,
- lesdits moyens de mise à jour de données accréditives sont adaptés pour générer et charger une nouvelle donnée accréditive dans lesdits premiers et seconds moyens de mémorisation consécutivement à une autorisation d'accès donnée par lesdits moyens de contrôle d'accès,
- lesdits moyens de gestion de données accréditives sont des moyens logiciels indépendants dudit logiciel,
- lesdits moyens de mise à jour de données accréditives sont adaptés pour générer et charger une nouvelle donnée accréditive dans lesdits premiers et seconds moyens de mémorisation consécutivement à une validation dudit code d'identification par lesdits moyens de validation,
- lesdits moyens de gestion de données accréditives comprennent des moyens pour dater et charger dans l'un au moins desdits moyens de mémorisation la date à laquelle une donnée accréditive est générée et des moyens inhibiteurs pour n'autoriser la génération d'une nouvelle donnée accréditive par lesdits moyens de mise à jour qu'après écoulement d'un délai

35

déterminé depuis la génération de ladite donnée accréditive stockée dans lesdits moyens de mémorisation,

- ledit logiciel est stocké et exécuté en totalité dans ledit terminal pour la mise en œuvre locale de ladite application,

5 - ledit système comprend au moins un serveur et des moyens de transmission de données entre ledit terminal et ledit serveur, ledit logiciel est stocké et exécuté pour partie dans ledit terminal et pour partie dans ledit serveur, et lesdits premiers moyens de mémorisation sont associés audit serveur.

10 D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre de différents modes de réalisation donnés uniquement à titre d'exemple et illustrés par les dessins annexés sur lesquels :

La figure 1 est un schéma bloc général d'un système informatique selon une première forme de réalisation de l'invention dans le cas d'une application exécutée pour partie dans un terminal et pour partie dans un serveur ;

15 La figure 2 est un schéma bloc d'un premier mode d'exécution du système informatique de la figure 1 ;

La figure 3 est un diagramme fonctionnel illustrant un premier mode de mise à jour des données accréditives dans le système informatique de la figure 2 ;

20 La figure 4 est un diagramme fonctionnel illustrant un deuxième mode de mise à jour des données accréditives dans le système informatique de la figure 2 ;

La figure 5 illustre un deuxième mode d'exécution du système informatique de la figure 1 ;

25 La figure 6 illustre un mode de mise à jour des données accréditives dans le système informatique de la figure 5 ;

La figure 7 illustre un troisième mode d'exécution du système informatique de la figure 1 ;

30 La figure 8 illustre un quatrième mode d'exécution du système informatique de la figure 1 ;

La figure 9 illustre un système informatique selon une deuxième forme de réalisation de l'invention dans laquelle une ou des applications sont exécutées localement dans un terminal ; et

35 La figure 10 illustre un mode de mise à jour des données accréditives dans le système informatique de la figure 9.

En se reportant à la figure 1, le système informatique représenté comprend un terminal T qui est connecté, d'une part à un dispositif de sécurité

personnel PSD et, d'autre part, à un système d'information I par l'intermédiaire d'un réseau R. Le dispositif de sécurité personnel PSD est relié au terminal T par des moyens L permettant d'assurer une transmission bidirectionnelle d'information entre eux.

5           Le terminal T peut être constitué, par exemple, par un ordinateur personnel, un téléphone, un téléphone mobile, un assistant numérique personnel, etc... Il est doté de manière conventionnelle de moyens d'interface avec l'utilisateur, de moyens de traitement de données (microprocesseur) et de  
10   ACC1, ACC2, ACCN, le terminal T est capable d'exécuter des applications A1, A2, ..... An en liaison, via le réseau R, avec des serveurs S<sub>1</sub>, S<sub>2</sub>, ..... S<sub>n</sub> contenant respectivement des logiciels ACS<sub>1</sub>, ACS<sub>2</sub>, ..... ACS<sub>n</sub>. Bien entendu, contrairement à ce qui a été représenté, chaque serveur S<sub>1</sub>, S<sub>2</sub>, ..... S<sub>n</sub> du système d'information I pourrait mettre en œuvre plusieurs applications. En  
15   résumé, les logiciels de chaque application sont distribués entre le terminal T et l'un des serveurs du système d'information I : le logiciel de l'application A1 est constitué par le logiciel ACC1 et ACS<sub>1</sub>, le logiciel de l'application A2 par le logiciel ACC2 et ACS<sub>2</sub>, le logiciel de l'application An par le logiciel ACCN et le logiciel ACS<sub>N</sub>.

20           Le réseau R assurant la transmission de données bidirectionnelles entre le terminal T et les serveurs S<sub>1</sub>, S<sub>2</sub> ..... S<sub>n</sub> du système d'information I peut être de nature quelconque, par exemple Internet.

          Au sens de la présente demande un dispositif de sécurité personnel PSD est un dispositif détenu et/ou accessible (par exemple par code PIN  
25   d'identification personnel ou autre) exclusivement par un utilisateur autorisé, et permettant d'y stocker de manière sécurisée des données en offrant des garanties de sécurité contre la lecture et/ou l'écriture de données par une personne non autorisée.

          Il peut s'agir, par exemple, d'une carte à puce, d'un dispositif portable  
30   électronique alimenté électriquement et comportant un nombre limité d'entrées et de sorties ainsi que des moyens de protection logiciels et matériels interdisant l'accès aux bus internes sur lesquels les données transitent dans le dispositif. Dans le cas d'une carte à puce, par exemple, les moyens de liaison L avec le terminal T sont constitués par un lecteur de carte à puce qui peut être  
35   extérieur ou intégré au terminal T.

          En variante, le dispositif de sécurité personnel peut être réalisé sous forme d'un logiciel implanté dans le terminal T et permettant de stocker des données de manière sécurisée dans le terminal, ces données pouvant

éventuellement être chiffrées. Ce mode de réalisation n'apporte pas le même degré de sécurité que celui offert par une carte à puce, mais il représente cependant une amélioration sensible dans la mesure où, comme cela sera expliqué dans la suite, les données accreditives de l'utilisateur peuvent être

5 modifiées automatiquement, et donc souvent.

Le dispositif de sécurité personnel PSD comprend une mémoire M dans laquelle sont stockées les données accreditives propres à l'utilisateur du terminal T et permettant à celui-ci de mettre en œuvre les différentes applications A1, A2 ..... An. Ces données accreditives attribuées à l'utilisateur

10 sont constituées par exemple d'un nom d'utilisateur et d'un mot de passe spécifique à l'application considérée.

Côté système d'information I, les différents serveurs S<sub>1</sub>, S<sub>2</sub>, ..... S<sub>n</sub> comprennent des fichiers F<sub>1</sub>, F<sub>2</sub>, ..... F<sub>n</sub> respectivement dans lesquels sont stockées les données accreditives de l'ensemble des utilisateurs autorisés à

15 accéder à une application mise en œuvre par le serveur considéré. C'est ainsi que les données accreditives de l'utilisateur du terminal T sont stockées dans la mémoire M et le fichier F<sub>1</sub> en ce qui concerne l'application A1, dans la mémoire M et le fichier F<sub>2</sub> en ce qui concerne l'application A2, dans la mémoire M et dans le fichier F<sub>n</sub> en ce qui concerne l'application An.

20 Bien entendu, le système informatique de la figure 1 peut comporter plusieurs terminaux T connectés par le réseau R au système d'information I et destinés à être utilisés par différents utilisateurs.

Afin d'exécuter une application (banque à domicile, commerce électronique, etc...), un utilisateur lance cette application sur son terminal T.

25 L'accès au dispositif de sécurité personnel PSD peut être subordonné à la fourniture par l'utilisateur d'un numéro d'identification personnel PIN via son terminal T. Une fois que la requête d'accès auprès du dispositif PSD a été acceptée, les données accreditives de l'utilisateur relatives à l'application considérée sont lues dans le dispositif de sécurité personnel PSD et sont

30 transmises au serveur considéré. Celui-ci compare les données accreditives reçues du terminal T à celles contenues dans son fichier de données accreditives et autorise l'exécution de l'application s'il y a concordance.

Afin d'assurer la gestion des données accreditives en vue d'une authentification vis-à-vis des applications A1, A2, ..... An, ainsi qu'une mise à

35 jour de ces données accreditives, il est prévu des moyens logiciels CMP de gestion des données accreditives. Ainsi que cela sera décrit dans la suite, ces moyens CMP sont distribués entre le terminal T et les serveurs S<sub>1</sub>, S<sub>2</sub>, ..... S<sub>n</sub> affectés aux différentes applications.



Pour assurer une authentification vis-à-vis d'une application donnée, il est nécessaire, au niveau du terminal T, de lire dans le dispositif de sécurité personnel PSD les données accréditives relatives à cette application.

- 5 Pour ce faire, il est possible de remplacer le logiciel d'application standard côté client ou terminal par un logiciel d'application modifié qui assure la gestion des communications avec le dispositif PSD en sus des caractéristiques standard de l'application. Ce type d'implantation correspond au mode d'exécution illustré par la figure 2.

- 10 Il est également possible d'utiliser un logiciel spécifique qui assure la lecture des données accréditives dans le dispositif PSD et les transmet à l'application considérée sans modification du logiciel d'application standard côté client ou terminal. Pour ce faire, il est possible de recourir à différentes solutions : émulation du clavier, envoi d'un message dans lequel les données accréditives sont contenues par exemple. Cette deuxième solution correspond  
15 aux formes d'exécution des figures 5, 7 et 8.

- On se reportera maintenant à la figure 2 sur laquelle, pour des raisons de simplicité, un seul serveur S a été représenté. Dans le mode d'exécution de la figure 2, le logiciel de gestion des données accréditives se présente, côté terminal, comme un logiciel d'application modifié côté client  $ACC_M$ . La partie de  
20 ce logiciel assurant la gestion des données accréditives est représentée par un cercle  $CMP_C$ . Côté serveur S, le logiciel de gestion des données accréditives est représenté par un cercle  $CMP_S$  : ce logiciel est celui qui existe de manière standard dans toute application pour permettre la modification des données accréditives des utilisateurs ou le chargement de données accréditives relatives  
25 à de nouveaux utilisateurs. Les logiciels  $CMP_C$  et  $CMP_S$ , qui font partie respectivement des logiciels  $ACC_M$  et  $ACS$ , forment ensemble le logiciel  $CMP$  de gestion des données accréditives de la figure 1.

- Selon l'implantation de la figure 2, les moyens logiciels de gestion des données accréditives intégrés à l'application A ont directement accès au  
30 dispositif de sécurité personnel PSD par l'intermédiaire du logiciel d'application modifié côté client  $ACC_M$ , et au fichier de données accréditives F du serveur S.

- En vue de permettre à un utilisateur exécutant l'application A de bénéficier d'une amélioration de la sécurité du processus d'authentification, un dispositif PSD dépourvu de données accréditives lui est remis par un  
35 administrateur de sécurité. Ce dispositif PSD ne contient aucun mot de passe statique.

L'utilisateur connecte son dispositif PSD à son terminal T et initialise dans celui-ci un numéro d'identification personnel PIN.

L'utilisateur installe ensuite le logiciel d'application modifié côté client ACC<sub>M</sub> à la place du logiciel d'application standard côté client utilisé jusqu'alors.

5 Lors de la première utilisation du logiciel ACC<sub>M</sub> pour accéder à l'application, l'utilisateur introduit son numéro d'identification personnel PIN pour autoriser l'accès au dispositif PSD et s'ouvre ensuite l'accès à l'application au moyen des données accréditives statiques connues de lui qu'il utilisait jusqu'alors avec son logiciel d'application standard côté client. Ces données accréditives en cours sont présentées au logiciel d'application côté serveur ACS au moyen du protocole d'authentification standard.

10 Une fois l'application côté serveur ouverte, la partie CMP<sub>c</sub> du logiciel d'application modifié côté client ACC<sub>M</sub> génère un mot de passe aléatoire, présente une requête de changement de mot de passe au logiciel CMP<sub>s</sub> côté serveur en lui transmettant le nouveau mot de passe, et charge alors les données accréditives statiques, comprenant le mot de passe généré ainsi  
15 éventuellement que le nom d'utilisateur, dans le dispositif PSD. Le nouveau mot de passe statique généré se trouve alors stocké dans le fichier F et dans la mémoire M tout en étant inconnu de l'utilisateur. Ce mécanisme permet d'utiliser des mots de passe forts, c'est-à-dire des mots de passe complexes (mots non compris dans un dictionnaire, difficiles à mémoriser et donc à imaginer, etc...) et  
20 comprenant un grand nombre de caractères, qui présentent une beaucoup plus grande résistance à des attaques que les mots de passe courts qui, en pratique, sont utilisés lorsqu'ils doivent être retenus ou introduits au clavier par un utilisateur.

Lors de l'accès suivant de l'utilisateur à l'application, il suffit à celui-ci  
25 d'introduire au terminal son numéro d'identification personnel PIN, le processus d'authentification étant ensuite assuré automatiquement par lecture des données accréditives dans le dispositif PSD et transmission de ces dernières via le logiciel CMP<sub>c</sub> au logiciel CMP<sub>s</sub> côté serveur. Pendant ce processus d'authentification, les données accréditives ne sont à aucun moment affichées  
30 sur l'écran du terminal T et demeurent donc inconnues de l'utilisateur, ce qui renforce la sécurité offerte par le système.

Ensuite, la mise à jour ou le changement du mot de passe statique peut être assurée à chaque accès à l'application considérée comme illustré à la figure 3, ou périodiquement, par exemple chaque jour, comme illustré à la figure  
35 4, ou bien encore sur une requête spécifique de l'administrateur système.

En se reportant à la figure 3, l'utilisateur formule en 1 une requête d'accès à une application X au niveau du terminal T et celle-ci est prise en compte en 2 au niveau du serveur S. L'utilisateur introduit en 3 son numéro ou

code d'identification personnel PIN via le terminal T et celui-ci est transmis au dispositif PSD qui effectue en 4 une comparaison du numéro introduit par l'utilisateur avec celui mémorisé en 5 dans le dispositif PSD.

5 Si le numéro PIN introduit par l'utilisateur ne correspond pas à celui mémorisé en 5, la requête d'accès est refusée au niveau du terminal en 6 ce qui conduit en 7 à l'abandon de la requête au niveau du serveur S.

10 Si la réponse au test 4 est positive, le dispositif PSD lit en 8 la donnée accréditive (mot de passe statique) mémorisée dans celui-ci pour l'application X et cette donnée est transmise via le terminal T au serveur S où une comparaison est effectuée en 9 avec la donnée accréditive (mot de passe statique) mémorisée dans le fichier F pour l'application X et l'utilisateur considéré (bloc 10). Si les données comparées en 9 ne concordent pas, l'accès à l'application X est refusé en 11. Dans le cas contraire, l'accès à l'application X est autorisé en 12 au niveau du serveur S et le terminal T génère en 13 une nouvelle donnée accréditive pour l'application X.

15 Cette nouvelle donnée accréditive (mot de passe généré aléatoirement) est transmise respectivement au serveur S et au dispositif PSD et en 14 et 15 elle est mémorisée respectivement dans le fichier F et dans la mémoire M. Le processus se termine en 16 et 17 par le déroulement ou exécution de l'application X respectivement au niveau du serveur S et du terminal T.

20 En variante, comme représenté à la figure 4, la modification ou mise à jour de la donnée accréditive (mot de passe statique) peut être subordonnée à l'écoulement d'un délai prédéterminé depuis le dernier changement de ce mot de passe. Le processus mis en œuvre est identique à celui de la figure 3 jusqu'à l'étape 12 et ne sera donc pas décrit à nouveau.

25 Après l'étape 12, le terminal T initie en 18 un processus de changement de donnée accréditive pour l'application X, ce qui conduit en 19 à la lecture dans le dispositif PSD de la date à laquelle la dernière donnée accréditive pour l'application X a été mémorisée dans le dispositif PSD. En 20, il est déterminé si un délai minimum, par exemple une journée, s'est écoulé depuis la dernière mise à jour de la donnée accréditive. Si tel n'est pas le cas, celle-ci n'est pas modifiée et l'on passe directement en 21 et 22 au déroulement ou à l'exécution de l'application dans le serveur S et le terminal T.

30 S'il est déterminé à l'étape 20 que le délai minimum imparti s'est écoulé, il est procédé en 23 au niveau du terminal T à la génération d'une nouvelle donnée accréditive pour l'application X et celle-ci est mémorisée en 24 et 25 respectivement dans le fichier F du serveur S et la mémoire M du dispositif

PSD, avec mémorisation de sa date de mise à jour au moins dans la mémoire M du dispositif PSD.

Le mode d'exécution de l'invention illustré par la figure 5 diffère de celui de la figure 2 en ce qui concerne le mode d'implantation des moyens logiciels de gestion des données accréditives. Côté terminal T, le logiciel de gestion des données accréditives fait partie d'un logiciel DD d'insertion de données ("Drag and Drop") qui est indépendant du logiciel d'application côté client ou terminal ACC. Côté système d'information I, il est prévu un module logiciel de gestion de données accréditives CMS indépendant du logiciel d'application côté serveur ACS et qui gère le fichier F des données accréditives associées au serveur S. Le module CMS peut être mis en œuvre dans le serveur S ou dans un serveur indépendant de celui-ci. Comme dans le cas de la figure 2, il doit être compris que la mise en œuvre de l'invention n'implique aucune modification matérielle et logicielle au niveau du système d'information I.

Dans la description qui va suivre, on supposera qu'un utilisateur du terminal T dispose déjà d'une autorisation d'accès à une application exécutée côté terminal par le logiciel d'application côté client ACC et côté serveur par le logiciel d'application côté serveur ACS. L'utilisateur est supposé également être en possession de données accréditives lui permettant de s'authentifier vis-à-vis de l'application et d'ouvrir celle-ci.

Afin de mettre en œuvre les mécanismes de sécurité améliorés suivant l'invention, l'utilisateur se voit doté par un administrateur de sécurité d'un dispositif PSD vierge, c'est-à-dire dépourvu de toutes données accréditives.

L'utilisateur connecte ensuite son dispositif PSD à son terminal T et installe le logiciel DD dans son terminal. De plus, il procède à l'initialisation du numéro d'identification personnel PIN commandant l'accès à son dispositif de sécurité personnel PSD.

Les anciennes données accréditives sont demandées à l'utilisateur et communiquées au module de gestion de données accréditives CMS par le logiciel DD afin d'authentifier l'utilisateur. De nouvelles données accréditives (mot de passe statique) sont générées par le logiciel DD et transmises au module CMS qui met à jour le fichier F de données accréditives, soit directement, soit par l'intermédiaire du logiciel ACS. Ces nouvelles données accréditives ne sont pas connues de l'utilisateur et peuvent comporter un mot de passe statique "fort" comme décrit précédemment.

Pour utiliser l'application, l'utilisateur lance le programme DD, introduit son numéro d'identification personnel PIN pour permettre l'accès au dispositif PSD et insère au niveau du logiciel ACC les données accréditives statiques

lues par le logiciel DD dans le dispositif PSD, par exemple par une opération de "glissé et lâché" (Drag and Drop) mise en œuvre par le logiciel DD au moyen d'une souris. Les mécanismes permettant par une opération de "glissé et lâché" d'introduire des données accréditives contenues dans un dispositif de sécurité personnel PSD dans un logiciel d'application sont décrites dans la demande de brevet français déposée par la Demanderesse le même jour que la présente demande pour " Dispositif informatique à accès par accréditation perfectionné", à laquelle on se référera pour plus de détails. Lors de ce chargement des données accréditives dans le logiciel d'application, celles-ci ne sont pas affichées sur l'écran du terminal et demeurent inconnues de l'utilisateur.

Le processus de mise à jour ou de modification des données accréditives sera maintenant décrit en regard du diagramme fonctionnel de la figure 6. Ce processus est mis en œuvre à chaque fois que l'utilisateur lance le logiciel DD sur le terminal T.

En 26, l'utilisateur requiert sur son terminal T un accès au logiciel DD. En 27, il introduit son numéro d'identification personnel PIN et, en 28, celui-ci est comparé dans le dispositif PSD avec le numéro d'identification personnel PIN qui s'y trouve mémorisé en 29. Si les deux numéros ne concordent pas, l'accès est refusé en 30. Si les deux numéros concordent, un processus de mise à jour des données accréditives de l'application X est initié en 31. Ce processus se traduit en 32, au niveau du module CMS, par une requête d'authentification de l'utilisateur pour l'application X et en 33 par une lecture des données accréditives de l'utilisateur actuellement stockées dans le fichier F pour l'application X.

Parallèlement, le processus initié en 31 conduit en 34 à la lecture dans le dispositif PSD des données accréditives de l'utilisateur pour l'application X et celles-ci sont transmises via le terminal R au module CMS.

En 35 une comparaison est effectuée dans celui-ci entre les données lues en 33 dans le fichier F et celles lues en 34 dans la mémoire M du dispositif PSD. En cas de discordance, l'authentification vis-à-vis du module CMS est refusée en 36 et il ne sera donc pas procédé à une modification des données accréditives.

Dans le cas contraire, il est procédé en 37 au niveau du terminal T, par le logiciel DD, à la génération d'une nouvelle donnée accréditive pour l'application X. Cette nouvelle donnée accréditive est mémorisée en 38 dans le fichier F via le module CMS et en 39 dans le dispositif PSD.

Si le dispositif PSD comprend des données accréditives relatives à plusieurs applications différentes, la partie  $CMP_T$  du logiciel DD initie ensuite en

40 un processus de mise à jour des données accréditives pour l'application Y, et ainsi de suite pour l'ensemble des applications pour lesquelles des données accréditives sont contenues dans le dispositif PSD.

- 5 Bien entendu, comme décrit en regard de la figure 4, la génération d'une nouvelle donnée accréditive (mot de passe statique) peut être subordonnée à l'écoulement d'un délai prédéterminé depuis la génération et la mémorisation de la donnée accréditive actuellement mémorisée dans le dispositif PSD.

- 10 Il est à noter que dans cette deuxième forme d'exécution de l'invention, la connexion du terminal T au module CMS n'est pas un préalable à l'accès à l'application. Celle-ci s'effectue comme décrit à propos de la figure 2 par envoi des données accréditives au logiciel d'application côté serveur ACS et, s'il ne peut pas être accédé au module CMS pour modifier les données accréditives, par exemple si le module CMS est mis en œuvre dans un autre serveur que le serveur S, l'accès à l'application supportée par le serveur S pourra néanmoins
- 15 être effectué grâce aux données accréditives non modifiées contenues dans la mémoire M et le fichier F. La mise à jours de ces données accréditives se trouvera simplement différée jusqu'à ce qu'une connexion avec le module CMS puisse être établie lors d'un nouveau lancement du programme DD. Le dispositif
- 20 passe qui nécessitent l'établissement préalable d'une connexion du terminal avec ce serveur de mot de passe pour permettre l'accès à une application.

La figure 7 illustre un mode d'exécution de l'invention qui diffère de celui de la figure 5 uniquement en ce qui concerne les moyens d'initialisation et de personnalisation du système.

- 25 Dans le système de la figure 7, il est prévu un outil de personnalisation T doté d'un logiciel de gestion de données accréditives  $CMP_P$  permettant à un administrateur de sécurité d'initialiser les données accréditives, relatives à un utilisateur pour une application donnée, dans le fichier F du serveur supportant l'application considérée et dans le dispositif de sécurité personnel PSD destiné
- 30 à l'utilisateur. Cela signifie que, outre les données accréditives initiales, le code d'identification personnel PIN est chargé dans le dispositif PSD au moyen de l'outil de personnalisation T. En variante, les données accréditives de l'utilisateur pour l'application considérée peuvent être initialisées ou mises à jour par l'administrateur de sécurité directement au moyen d'outils d'administration
- 35 standards prévus pour définir les droits de l'utilisateur vis-à-vis de l'application.

Dans une deuxième phase, le dispositif PSD et le code PIN qui lui est associé sont remis à l'utilisateur par des canaux séparés comme cela est classique, notamment en matière de carte à puce.

Ensuite, l'utilisateur connecte son dispositif PSD à son terminal T et charge le logiciel DD dans son terminal.

Pour accéder à une application, l'utilisateur lance le logiciel DD, introduit son code PIN pour permettre l'accès au dispositif PSD puis, comme décrit  
5 précédemment à propos de la figure 5, grâce au logiciel DD, introduit dans le logiciel ACC les données accréditives lues dans le dispositif PSD par une opération de "glissé-lâché" au moyen d'une souris.

Pour le reste, la mise à jours des données accréditives est effectuée périodiquement comme décrit à propos de la figure 5.

10 Il est à noter qu'en variante ce processus d'initialisation et de personnalisation pourrait être également mis en œuvre dans le cas d'une architecture matérielle et logicielle telle que décrite à la figure 2, c'est-à-dire dans le cas où le logiciel de gestion de données accréditives fait partie intégrante du logiciel d'application côté client ACC<sub>M</sub> et côté serveur ACS.

15 La figure 8 illustre une variante d'exécution du processus d'initialisation et de personnalisation de la figure 7.

Dans le cas de la figure 8, les données accréditives des utilisateurs sont générées par un outil de personnalisation sous la commande d'un administrateur de sécurité et sont stockées, pour chaque utilisateur, dans un  
20 fichier de données accréditives initiales K associé au module de gestion de données accréditives CMS. Un dispositif PSD vierge, c'est-à-dire ne contenant aucune donnée accréditive, est remis à l'utilisateur par l'administrateur de sécurité. Par un canal séparé, un mot de passe d'authentification initial, également stocké dans le fichier K, est transmis à l'utilisateur.

25 Celui-ci connecte le dispositif PSD qu'il a reçu au terminal T et installe si nécessaire le logiciel DD. D'autre part, l'utilisateur affecte un numéro d'identification personnel PIN à son dispositif PSD. L'utilisateur se connecte ensuite au module de gestion de données accréditives CMS au moyen du logiciel DD et s'authentifie vis-à-vis de celui-ci en présentant le mot de passe  
30 d'authentification initial qui lui a été communiqué. Une fois l'utilisateur authentifié, le module CMS charge dans le logiciel DD les données accréditives initiales stockées pour l'utilisateur considéré dans le fichier K. Ces données accréditives initiales sont transférées par le logiciel DD au dispositif PSD où elles sont mémorisées. Parallèlement, les données accréditives initiales de  
35 l'utilisateur sont chargées par le module CMS dans le fichier F, ou mises à jour dans celui-ci si l'utilisateur était déjà accrédité pour l'application considérée.

Ensuite, comme décrit en regard des figures 5 à 7, il suffit à l'utilisateur, pour s'authentifier vis-à-vis de l'application, d'introduire son code PIN puis de

charger dans le logiciel ACC, au moyen du logiciel DD, les données  
accréditives lues par ce dernier dans le dispositif PSD. Bien entendu, comme  
dans les exemples précédents, lors de ce chargement des données accréditives  
par une opération de "glissé-lâché" au moyen de la souris et du logiciel DD, les  
5 données accréditives proprement dites ne sont pas affichées sur l'écran du  
terminal et ne sont donc pas connues de l'utilisateur.

Après initialisation et personnalisation, la mise à jours des données  
accréditives s'opère comme décrit en regard des figures 5 et 7.

La figure 9 illustre une deuxième forme de réalisation de l'invention dans  
laquelle l'application est exécutée de façon purement locale dans le terminal T  
au moyen d'un logiciel d'application LA chargé dans celui-ci. Dans ce cas, le  
fichier F des données accréditives est stocké en mémoire dans le terminal T. Le  
logiciel CMP de gestion de données accréditives est également exécuté en  
local et fait partie du logiciel DD d'insertion de données. Ce logiciel CMP a  
15 directement accès au dispositif de sécurité personnel PSD, et accès au fichier  
F, soit directement comme représenté, soit par l'intermédiaire du logiciel  
d'application LA.

Initialement, un dispositif PSD vierge dépourvu de toute donnée  
accréditive est remis à l'utilisateur par un administrateur de sécurité.

20 L'utilisateur connecte son dispositif PSD à son terminal T, charge le  
logiciel DD et affecte un code d'identification personnel PIN à son dispositif  
PSD.

Les anciennes données accréditives de l'utilisateur pour l'application LA  
sont ensuite requises dans le logiciel DD pour authentifier l'utilisateur. Le  
25 logiciel DD génère de nouvelles données accréditives qui sont chargées dans le  
dispositif PSD et viennent remplacer les anciennes données accréditives dans  
le fichier F, soit directement, soit par l'intermédiaire de l'application LA.

Pour accéder à l'utilisation LA, il suffit ensuite à l'utilisateur de lancer le  
programme DD, d'introduire son code PIN permettant l'accès au dispositif PSD  
et de charger les données accréditives dans le logiciel d'application LA par une  
30 opération de "glissé-lâché" comme décrit en regard des figures 5, 7 et 8, étant  
entendu là encore que les données accréditives ne sont pas affichées à l'écran  
au cours de cette opération et demeurent par conséquent inconnues de  
l'utilisateur.

35 Le processus de mise à jour des données accréditives dans le cadre du  
système informatique de la figure 9 est illustré par le diagramme fonctionnel de  
la figure 10.



Après avoir requis en 41a un accès au logiciel DD, l'utilisateur introduit son code PIN en 41b au niveau du terminal T et celui-ci est transmis au dispositif PSD qui procède en 42 à une comparaison avec le code PIN qui s'y trouve mémorisé en 43. En cas de discordance, la requête est rejetée en 44.

- 5 Dans le cas contraire, le logiciel DD initie en 45 un processus de mise à jour des données accréditives pour l'application X. A cet effet, il lit en 46 les données accréditives stockées pour l'application X dans le fichier F et en 47 celles stockées pour cette même application X dans le dispositif PSD. Ces données accréditives sont comparées en 48 et, en cas de discordance, la modification des données est refusée en 49.

10 Dans le cas contraire, le logiciel DD génère en 50 une nouvelle donnée accréditive pour l'application X et celle-ci est stockée en 51 dans le fichier F et en 52 dans le dispositif PSD.

- 15 Si le terminal T est équipé de logiciels pour plusieurs applications X, Y, etc....., un nouveau processus de mise à jour des données accréditives pour l'application Y est initié en 53, et ainsi de suite pour l'ensemble des applications.

- Il résulte de ce qui précède que le système décrit permet l'authentification d'utilisateurs au moyen de données accréditives statiques, et notamment d'un mot de passe statique, qui demeurent inconnues de l'utilisateur.
- 20 Celui-ci n'a donc pas à se souvenir d'un mot de passe et n'est donc pas tenté de l'écrire en un lieu quelconque pour s'en souvenir.

Ce mot de passe statique peut être complexe et avoir la longueur maximale compatible avec l'application considérée étant donné qu'il n'a pas à être mémorisé par l'utilisateur et introduit par celui-ci dans son terminal.

- 25 De plus, ce mot de passe statique est mis à jour périodiquement de manière automatique, c'est-à-dire que cette mise à jour n'est pas soumise à la discrétion de l'utilisateur. Ce mot de passe statique "fort" et renouvelé périodiquement est stocké dans un dispositif de sécurité personnel à l'utilisateur, du type carte à puce ou similaire ou du type purement logiciel, qui
- 30 offre un degré de protection très élevé contre les tentatives de lecture illicites des données qui y sont contenues.

- Enfin, pour accéder à une application, le système décrit ne nécessite la connexion en temps réel du terminal à aucun serveur autre que celui sur lequel l'application est éventuellement en partie exécutée. En effet, si dans les modes
- 35 de réalisation des figures 5, 7 et 8, le module CMS de gestion des données accréditives peut être implanté dans un serveur indépendant de celui dans lequel l'application est pour partie exécutée, il n'en demeure pas moins que la connexion à ce serveur indépendant n'est pas nécessaire pour accéder à

l'application. Le système décrit se différencie donc fondamentalement des systèmes à serveur de mot de passe.

5 D'autre part, le système décrit n'entraîne aucune modification au niveau des serveurs existants, les seules modifications nécessaires concernant les logiciels à implanter dans le ou les terminaux. Le système informatique décrit permet donc de renforcer considérablement la sécurité de systèmes existants faisant appel à une authentification par données accréditives statiques pour accéder à une ou des applications.

10 Il va de soi que les modes de réalisation décrits ne sont que des exemples et l'on pourrait les modifier, notamment par substitution d'équivalents techniques, sans sortir pour cela du cadre de l'invention. C'est ainsi, par exemple, que la mise à jour des données accréditives pourrait être effectuée, non pas comme décrit lors de chaque accès à une application ou après écoulement d'un délai prédéterminé, mais en fonction d'un nombre  
15 d'événements. Un compteur peut être incrémenté à chaque requête d'authentification ou à chaque accès aux données accréditives. Lors de chaque requête d'authentification ou de chaque accès aux données accréditives, le contenu de ce compteur est comparé à une valeur de seuil, et si celle-ci est atteinte, les données accréditives sont modifiées. Ce seuil peut être choisi pour  
20 que la mise à jour des données accréditives ait lieu lors de chaque authentification réussie auprès d'une application comme décrit en regard de la figure 6.

Il doit être compris que l'expression "données accréditives" utilisée dans la description et les revendications désigne aussi bien les données accréditives  
25 proprement dites (mot de passe, nom d'utilisateur,.....) servant à s'authentifier vis-à-vis d'une application qu'une ou des clés secrètes ou privées de calcul d'une ou plusieurs données accréditives proprement dites. La mise à jour des "données accréditives" dont il est question dans ce qui précède peut donc, suivant les cas, concerner des données accréditives proprement dites et/ou des  
30 clés secrètes ou privées de calcul de données accréditives proprement dites.

### REVENDEICATIONS

1. Système informatique pour l'exécution d'au moins un logiciel dont l'accès par un utilisateur est commandé par la fourniture d'au moins une donnée accréditive attribuée audit utilisateur, ledit système comprenant :

- 5           - au moins un terminal comportant des moyens de traitement de données pour l'exécution dudit logiciel au moins en partie,
- des premiers moyens de mémorisation associés audit logiciel pour le stockage d'au moins une première donnée accréditive propre audit utilisateur,
- des moyens de contrôle d'accès pour autoriser l'accès audit logiciel en
- 10   réponse à une cohérence entre ladite première donnée accréditive stockée dans lesdits premiers moyens de mémorisation et une seconde donnée accréditive appliquée via ledit terminal audit logiciel,
- caractérisé en ce que ledit système comprend :
  - au moins un dispositif de sécurité (PSD) personnel audit utilisateur,
  - 15   associé audit terminal, et comportant des seconds moyens de mémorisation (M) pour le stockage sécurisé de ladite seconde donnée accréditive, et
  - et en ce que ledit terminal (T) comprend au moins en partie des moyens de gestion de données accréditives (CMP) comportant :
    - des moyens de lecture et de transmission de donnée accréditive pour
    - 20   lire ladite seconde donnée accréditive stockée dans lesdits seconds moyens de mémorisation (M) et la transmettre auxdits moyens de contrôle d'accès en réponse à la présentation d'une demande d'accès audit logiciel, et
    - des moyens de mise à jour de données accréditives pour commander
    - sélectivement la génération et le chargement dans lesdits premiers (F) et lesdits
    - 25   seconds (M) moyens de mémorisation respectivement d'une nouvelle donnée accréditive en remplacement de la donnée accréditive précédemment mémorisée.

2. Système selon la revendication 1, caractérisé en ce que lesdits moyens de contrôle d'accès (9) sont adaptés pour autoriser l'accès audit logiciel

30   en réponse à une identité entre lesdites première et seconde données accréditives.

3. Système selon l'une quelconque des revendications 1 et 2, caractérisé en ce que lesdits seconds moyens de mémorisation (M) sont adaptés pour stocker un premier code d'identification dudit utilisateur, ledit terminal (T)

35   comprend des moyens d'interface pour l'application d'un second code d'identification audit dispositif de sécurité personnel (PSD), l'accès audit dispositif personnel de sécurité étant autorisé en réponse à une identité entre lesdits premier et second codes d'identification (PIN).

4. Système selon l'une quelconque des revendications 1 à 3, caractérisé en ce que lesdits moyens de mise à jour de données accréditives sont adaptés pour générer automatiquement et transmettre ladite nouvelle donnée accréditive directement auxdits premiers (F) et seconds moyens de mémorisation (M), sans communication de ladite nouvelle donnée accréditive audit utilisateur.
- 5 5. Système selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdits moyens de gestion de données accréditives (CMP) sont des moyens logiciels faisant partie dudit logiciel (ACC1, ACS1 ; ACC2.....).
- 10 6. Système selon la revendication 5, caractérisé en ce que lesdits moyens de mise à jour de données accréditives (CMP) sont adaptés pour générer et charger une nouvelle donnée accréditive dans lesdits premiers (F) et seconds (M) moyens de mémorisation consécutivement à une autorisation d'accès donnée par lesdits moyens de contrôle d'accès.
- 15 7. Système selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdits moyens de gestion de données accréditives (CMP) sont des moyens logiciels indépendants dudit logiciel (ACC, ACS).
- 20 8. Système selon les revendications 3 et 7, caractérisé en ce que lesdits moyens de mise à jour de données accréditives (CMP) sont adaptés pour générer et charger une nouvelle donnée accréditive dans lesdits premiers (F) et seconds (M) moyens de mémorisation consécutivement à une validation dudit code d'identification par lesdits moyens de validation.
- 25 9. Système selon l'une quelconque des revendications 6 et 8, caractérisé en ce que lesdits moyens de gestion de données accréditives (CMP) comprennent des moyens pour dater et charger dans l'un au moins desdits moyens de mémorisation (M) la date à laquelle une donnée accréditive est générée et des moyens inhibiteurs (20) pour n'autoriser la génération d'une nouvelle donnée accréditive par lesdits moyens de mise à jour qu'après écoulement d'un délai déterminé depuis la génération de ladite donnée accréditive stockée dans lesdits moyens de mémorisation (M).
- 30 10. Système selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ledit logiciel est stocké et exécuté en totalité dans ledit terminal (T) pour la mise en œuvre locale de ladite application.
- 35 11. Système selon l'une quelconque des revendications 1 à 9, caractérisé en ce qu'il comprend au moins un serveur (S) et des moyens (R) de transmission de données entre ledit terminal (T) et ledit serveur, en ce que ledit logiciel est stocké et exécuté pour partie dans ledit terminal (T) et pour partie dans ledit serveur (S), et en ce que lesdits premiers moyens de mémorisation (F) sont associés audit serveur (S).

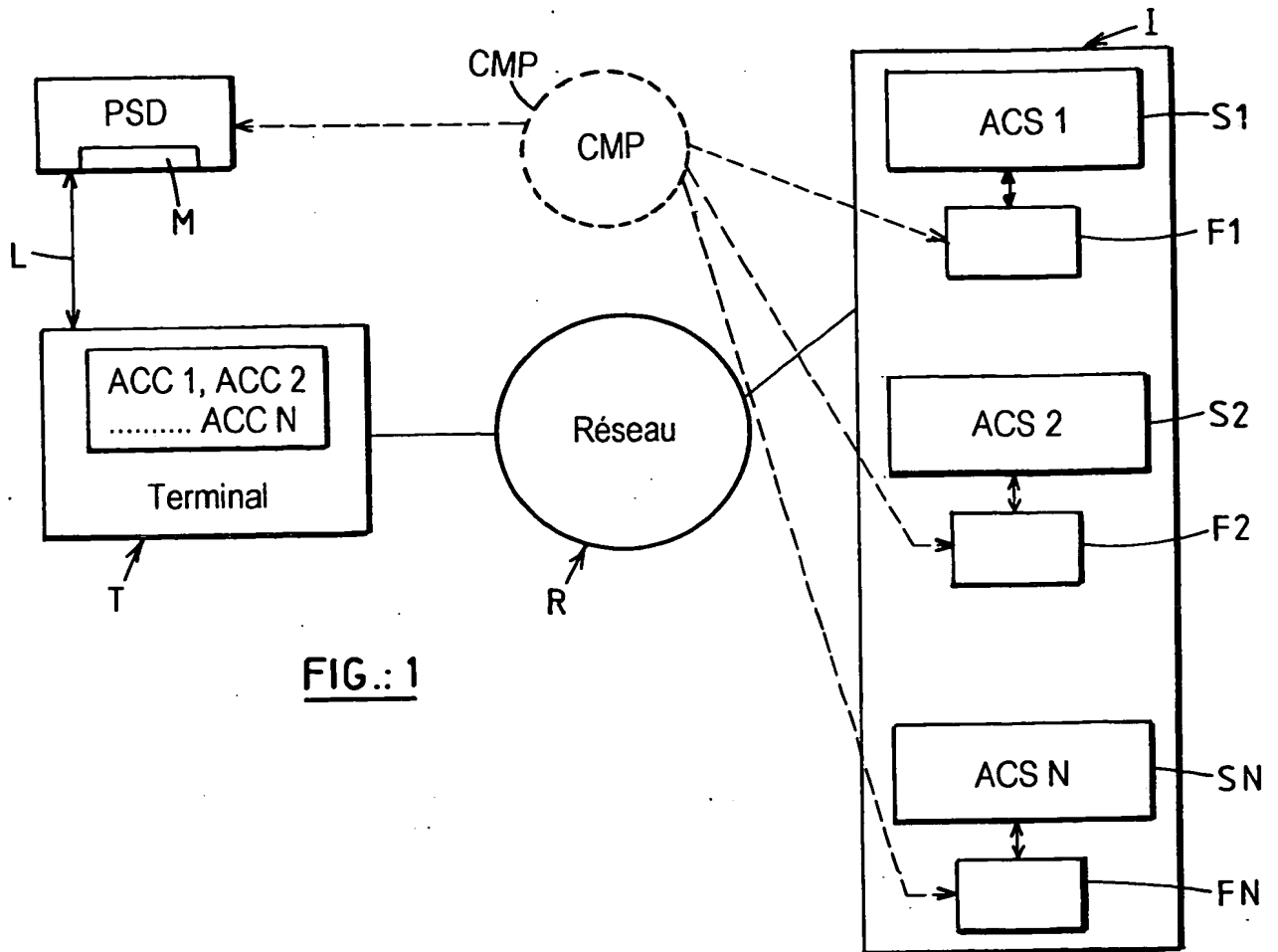


FIG.: 1

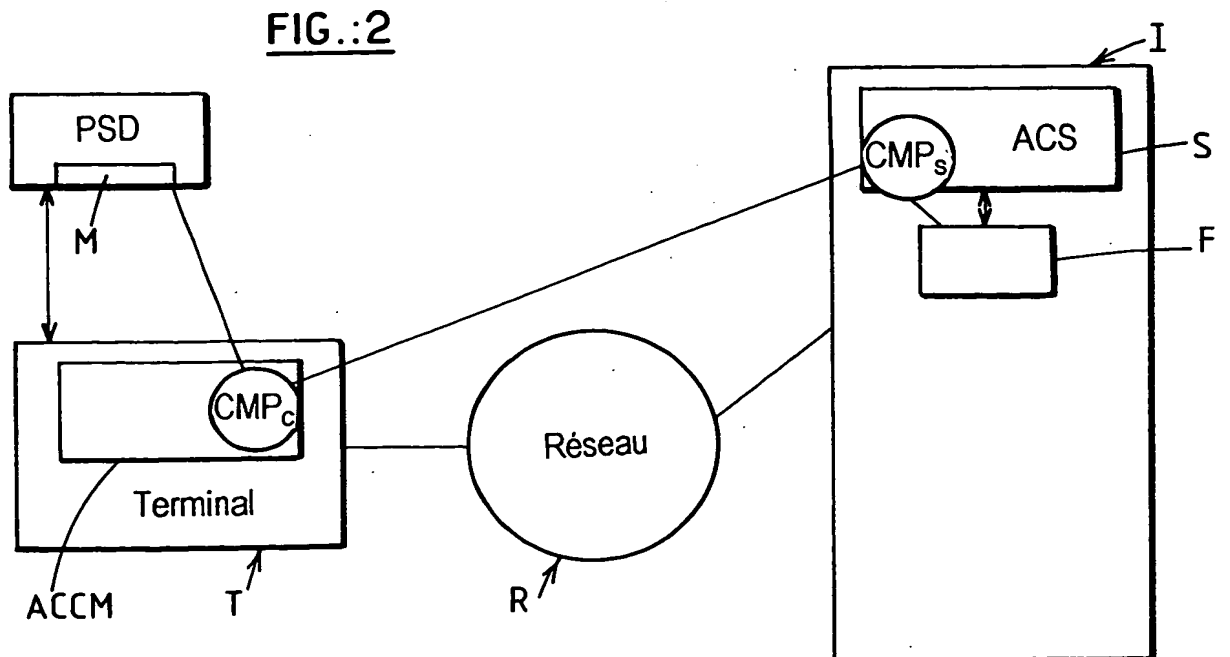
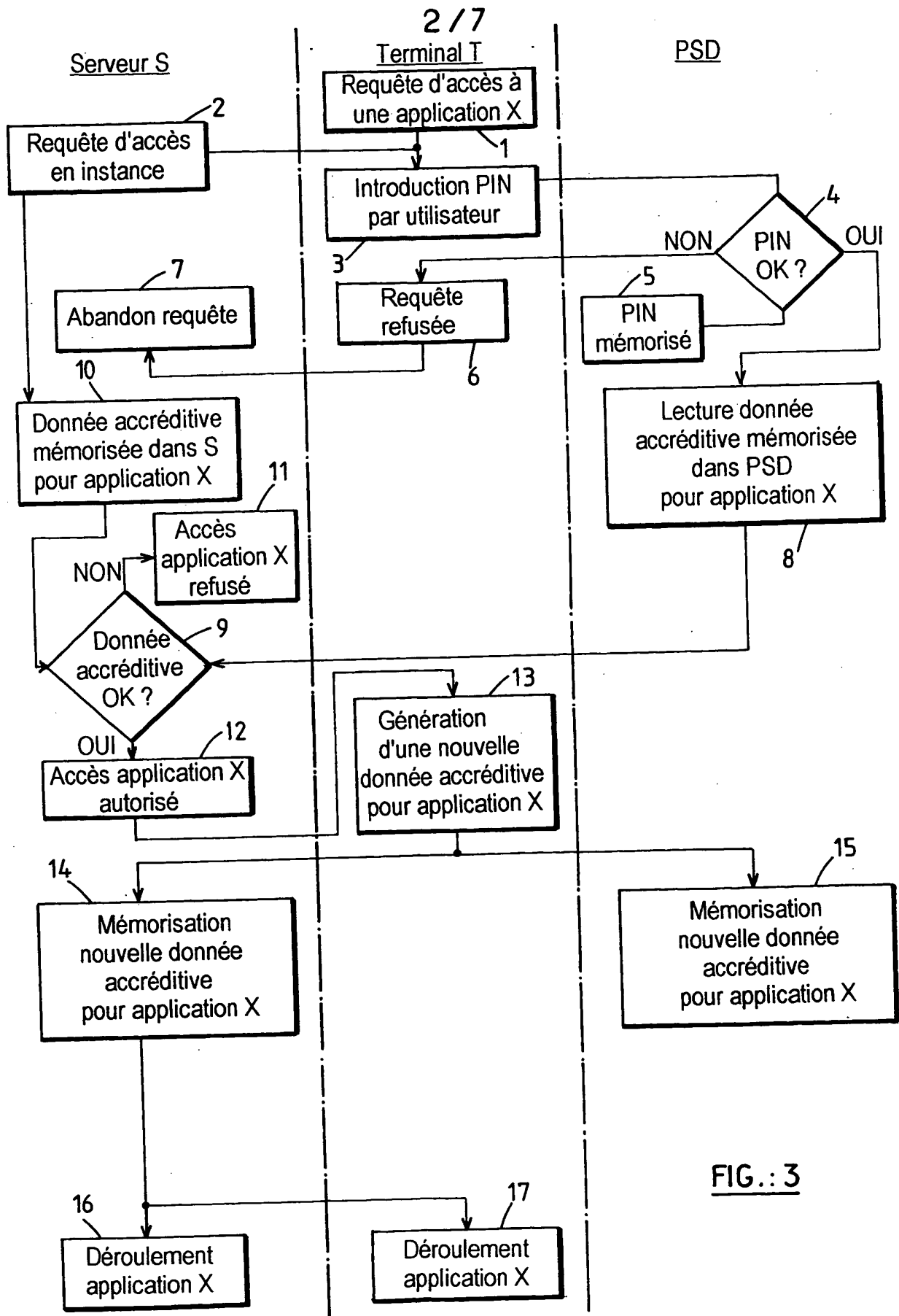


FIG.: 2



**FIG.: 3**

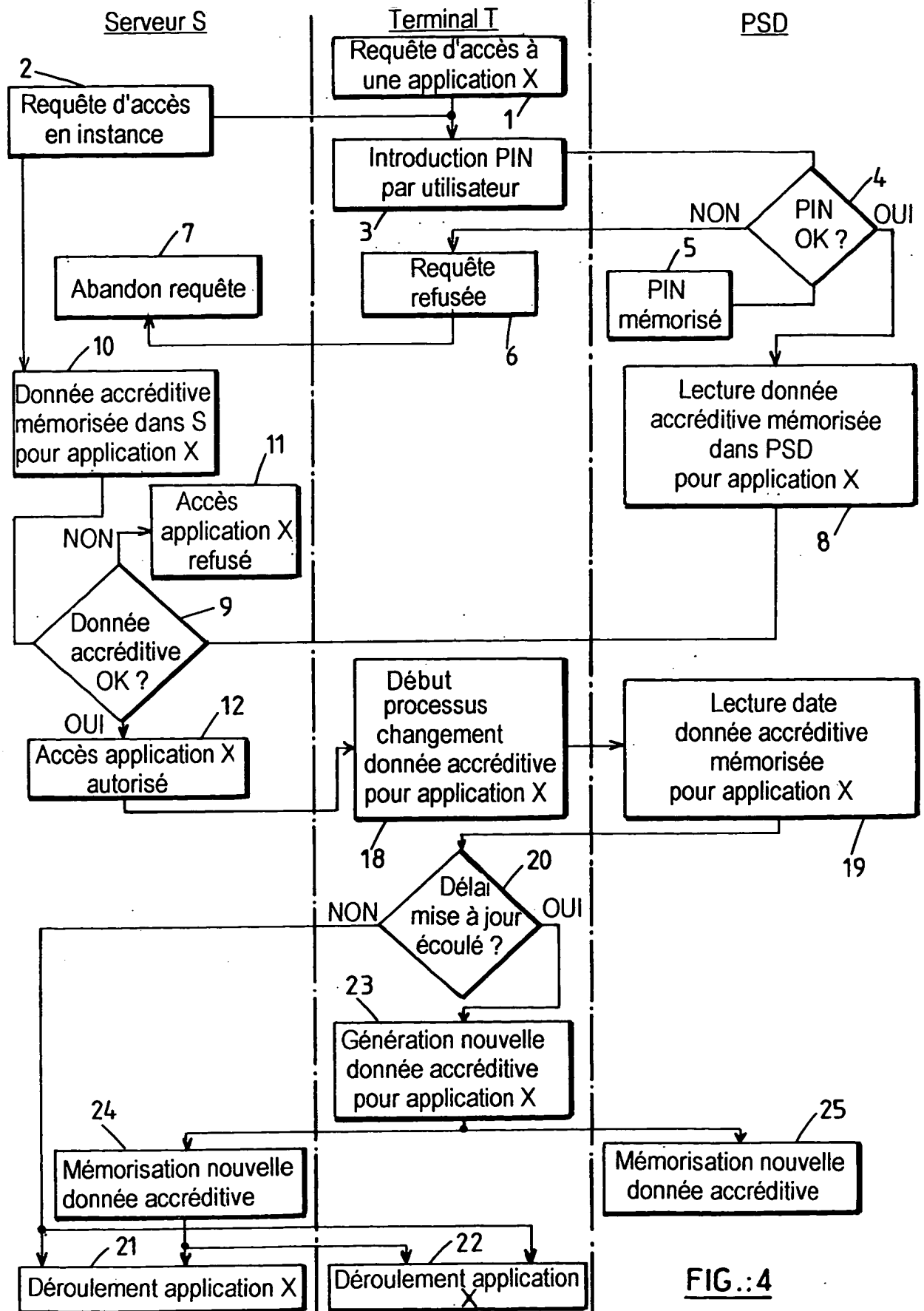
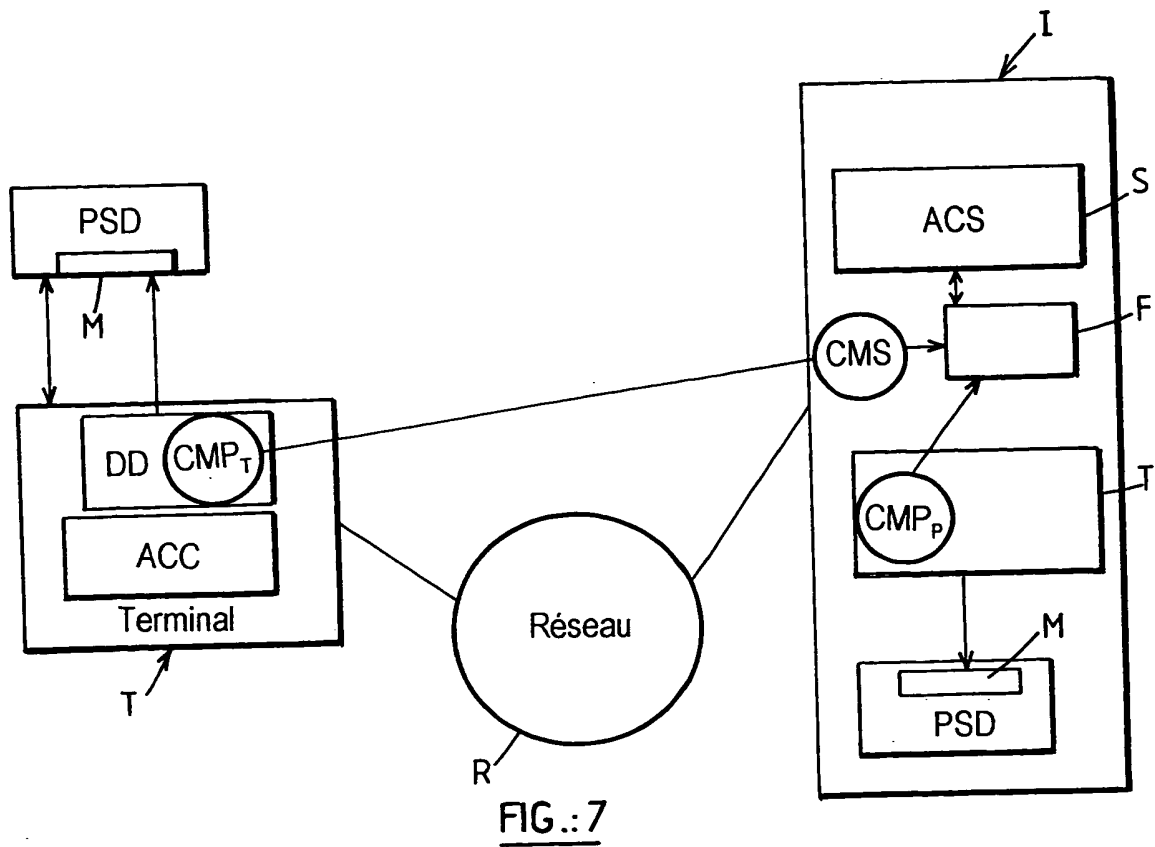
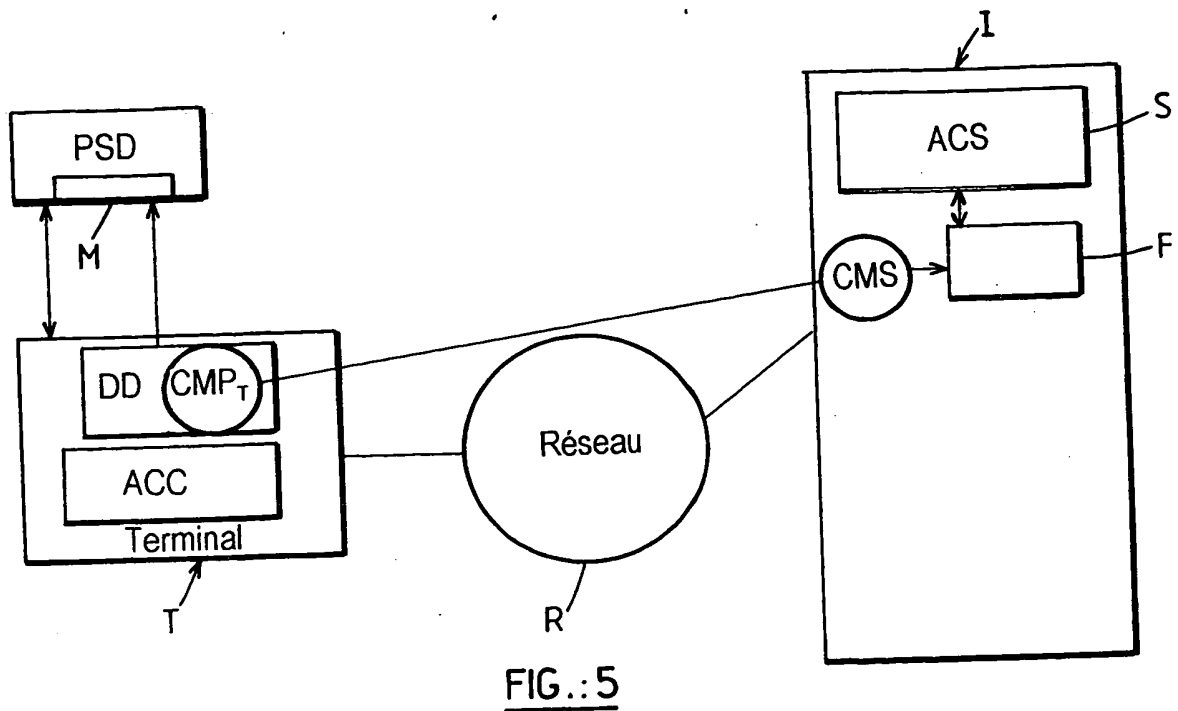


FIG.:4





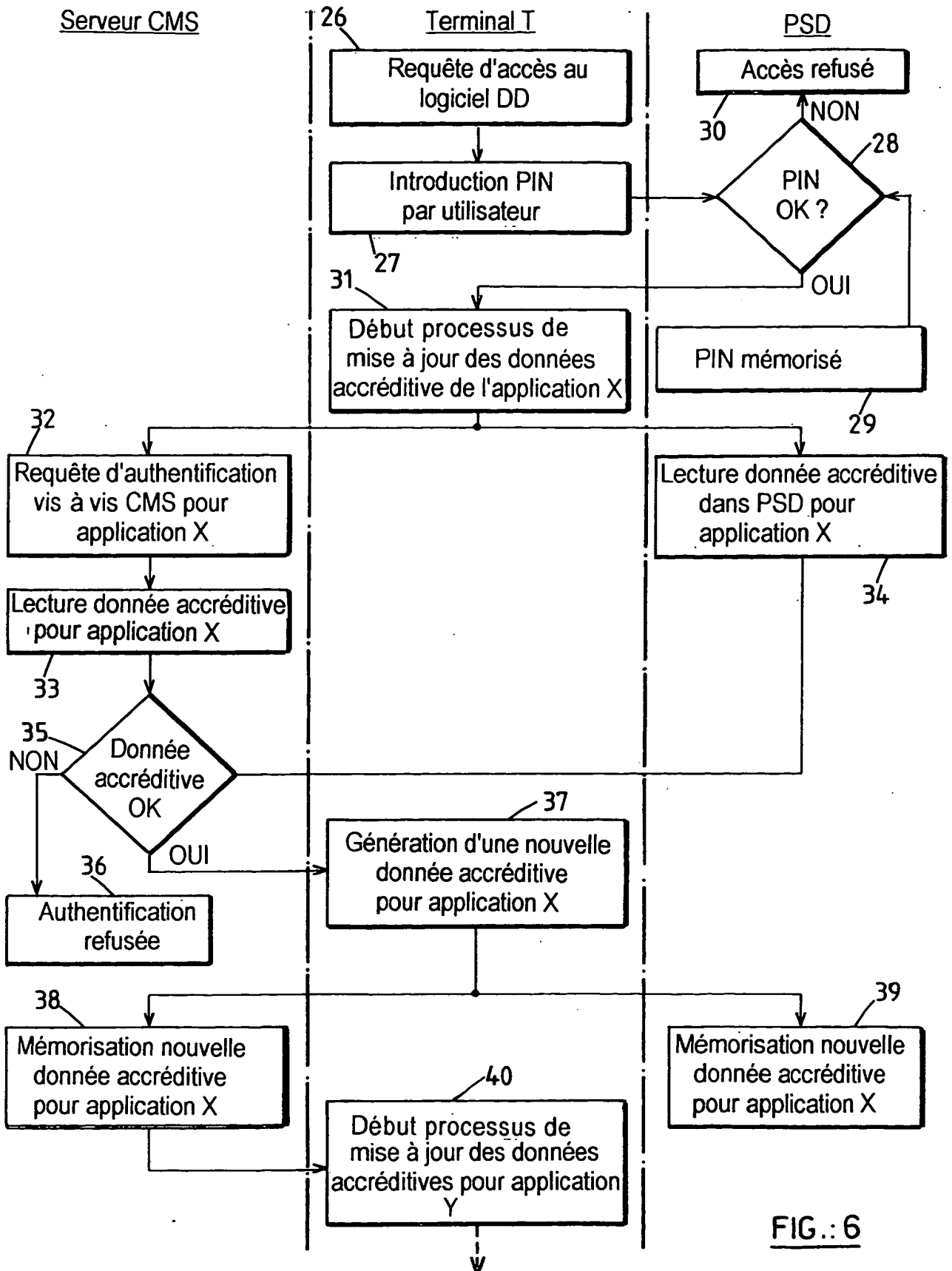
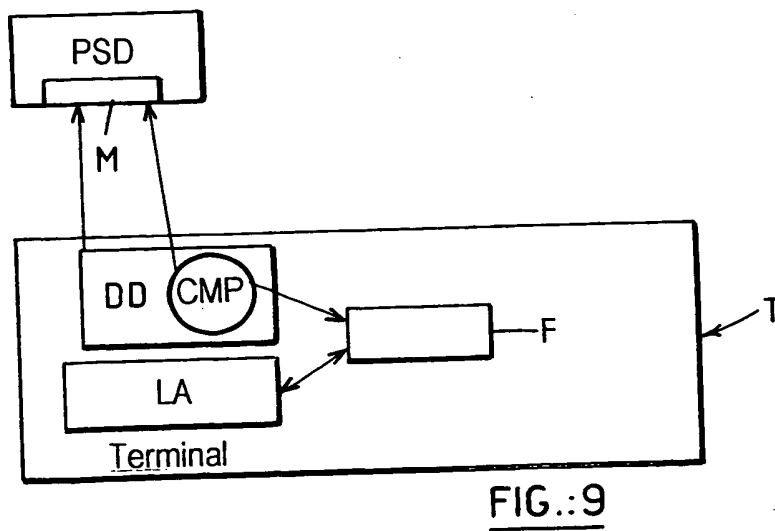
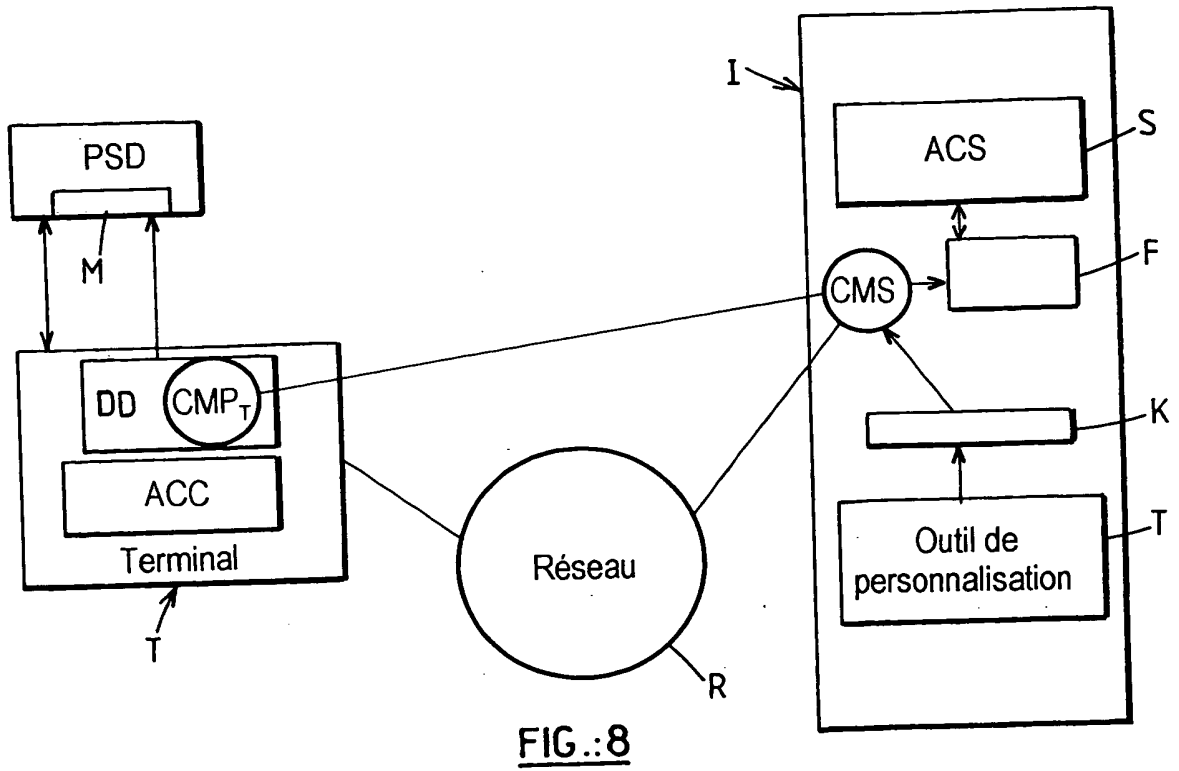


FIG.: 6



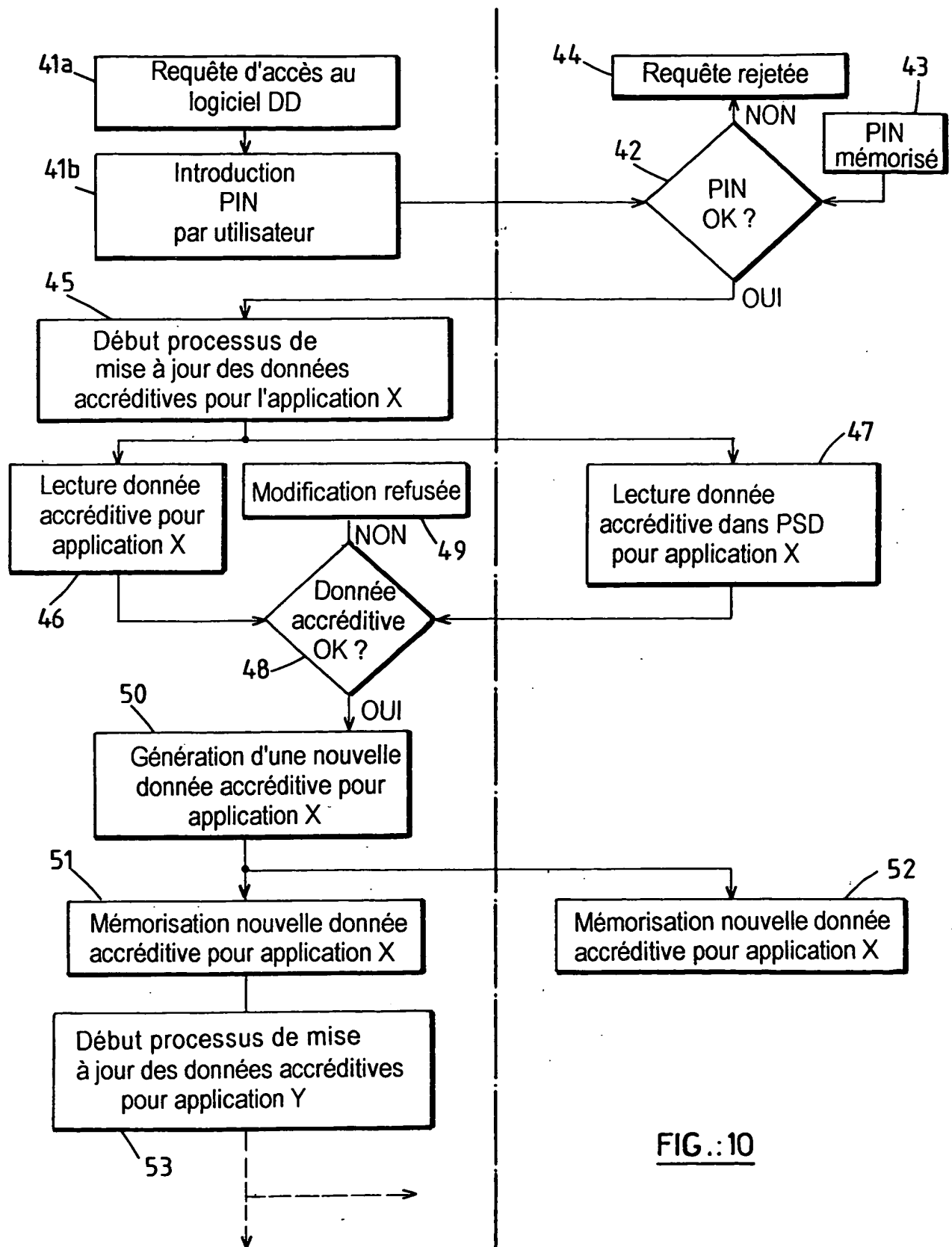


FIG.: 10

*This Page Blank (uspto)*

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**This Page Blank (uspto)**